

METHOD FOR INSPECTING ON-VEHICLE CONTROL UNIT

Publication number: JP2001202266 (A)

Publication date: 2001-07-27

Inventor(s): NAKAYAMA KIYONARI; KAMIYA KENJI; AOKI CHIZURU +

Applicant(s): DENSO CORP +

Classification:

- **international:** G06F11/22; G06F11/00; G06F11/22; G06F11/00; (IPC1-7): G06F11/22; G06F11/00

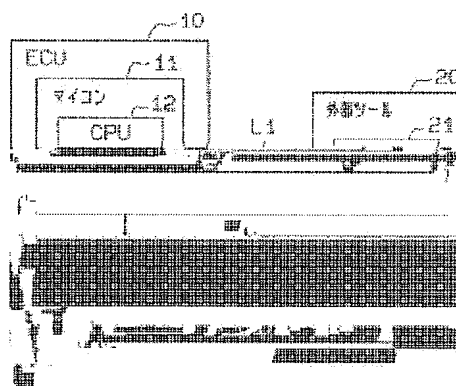
- **European:**

Application number: JP20000012803 20000121

Priority number(s): JP20000012803 20000121

Abstract of JP 2001202266 (A)

PROBLEM TO BE SOLVED: To rightly inspect an on-vehicle control unit and to prevent illegal alteration as the result. **SOLUTION:** An ECU 10 is provided with a widely known microcomputer 11, which is provided with a CPU 12 forming the center of various kinds of control, a flash memory 13 which can be erased and written electrically, and the other input/output circuit, etc., not shown in the figure. An external tool 20 is also provided with a widely known microcomputer 11 consisting of a CPU, a memory, an input/output circuit, etc. On judging (inspecting) the authenticity of the ECU 10, the tool 20 first transmits transmission data including a sum value calculation command and a random number to the ECU 10. The ECU 10 calculates the sum value of data in the memory 13 and enciphers the sum value in accordance with the random number by using a prescribed enciphering algorithm. After then, the enciphered sum value is transmitted to the tool 20, which compares and judges a decoded sum value and a previously registered true sum value to judge whether the ECU 10 is normal or abnormal by the result of it.



Data supplied from the **espacenet** database — Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-202266
(P2001-202266A)

(43) 公開日 平成13年7月27日 (2001.7.27)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 0 6 F 11/22	3 4 0	G 0 6 F 11/22	3 4 0 B 5 B 0 4 8
	3 1 0		3 1 0 F
11/00	3 4 0	11/00	3 4 0

審査請求 未請求 請求項の数6 O L (全 12 頁)

(21) 出願番号 特願2000-12803(P2000-12803)

(22) 出願日 平成12年1月21日 (2000.1.21)

(71) 出願人 000004260

株式会社デンソー

愛知県刈谷市昭和町1丁目1番地

(72) 発明者 中山 聖也

愛知県刈谷市昭和町1丁目1番地 株式会
社デンソー内

(72) 発明者 神谷 健治

愛知県刈谷市昭和町1丁目1番地 株式会
社デンソー内

(74) 代理人 100068755

弁理士 恩田 博宣 (外1名)

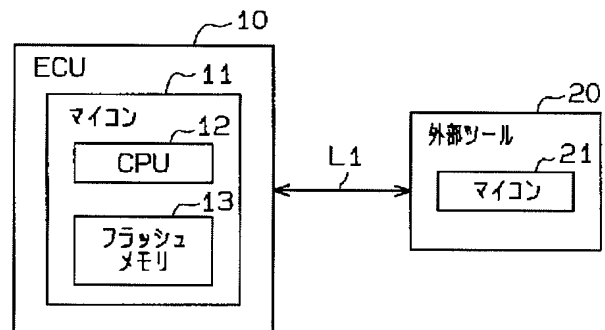
最終頁に続く

(54) 【発明の名称】 車載制御ユニットの検査方法

(57) 【要約】

【課題】 車載制御ユニットを正しく検査し、ひいては不正改造の防止を図る。

【解決手段】 ECU 10 は周知のマイコン 11 を備え、マイコン 11 は、各種制御の中核をなす CPU 12、電氣的に消去及び書き込み可能なフラッシュメモリ 13、その他図示しない入出力回路等を備える。外部ツール 20 も同様に、CPU、メモリ、入出力回路等からなる周知のマイコン 21 を備える。ECU 10 の正偽判定 (検査) に際し、外部ツール 20 では先ず、サム値算出指令と乱数とを含む送信データを ECU 10 に送信する。ECU 10 では、フラッシュメモリ 13 内のデータのサム値を算出すると共に、所定の暗号化アルゴリズムを用い、乱数に応じてサム値を暗号化する。その後、暗号化サム値を外部ツール 20 に送信する。外部ツール 20 では、復号化したサム値と予め登録されている真のサム値とを比較判定し、その結果により ECU 10 が正常か異常かを判断する。



【特許請求の範囲】

【請求項1】車載制御ユニット内のメモリについてデータのサム値を求め、該サム値により本制御ユニットを検査する車載制御ユニットの検査方法において、乱数を発生させ、その乱数をサム値の算出指令と共に外部ツールから制御ユニットへ送信する第1のステップと、

前記メモリのサム値を算出すると共に、該サム値を前記乱数に応じて暗号化する第2のステップと、
前記暗号化したデータを外部ツールに送信する第3のステップと、

外部ツールで受信したデータを復号化すると共に、そのデータ中のサム値を予め用意された真のサム値と比較し、その比較判定の結果から車載制御ユニットを検査する第4のステップと、からなることを特徴とする車載制御ユニットの検査方法。

【請求項2】車載制御ユニット内のメモリは、電氣的に書き換え可能な不揮発性メモリである請求項1に記載の車載制御ユニットの検査方法。

【請求項3】前記第4のステップにおいてサム値が不一致となった場合、前記第1のステップに戻って新たに乱数を設定し、それに続く第2～第4のステップを再度実施する請求項1又は2に記載の車載制御ユニットの検査方法。

【請求項4】複数の暗号化アルゴリズムを車載制御ユニットに予め用意しておく、

前記第1のステップでは、複数の暗号化アルゴリズムの中から一つを指定してそれを表す識別データを、乱数とサム値の算出指令と共に外部ツールから制御ユニットへ送信し、

前記第2のステップでは、前記識別データによる指定通りの暗号化アルゴリズムを使って暗号化を行い、その後、前記第4のステップでは、前記指定した暗号化アルゴリズムに対応する復号化の算出式を取り出して受信データを復号化し、サム値を抽出する請求項1又は2に記載の車載制御ユニットの検査方法。

【請求項5】車載制御ユニットは、電氣的に書き換え可能な不揮発性メモリを実装した第1マイクロコンピュータと、書き換え不可能なROMを実装した第2マイクロコンピュータとを備え、第2マイクロコンピュータのROMに、前記不揮発性メモリのサム値を暗号化するための暗号化アルゴリズムを記憶させておく請求項1～4の何れかに記載の車載制御ユニットの検査方法。

【請求項6】請求項5に記載の車載制御ユニットの検査方法において、

前記第2のステップは、前記不揮発性メモリのサム値を第1マイクロコンピュータから第2マイクロコンピュータへ送信するステップと、第2マイクロコンピュータにて前記ROM内の暗号化アルゴリズムでサム値を暗号化した後、その暗号化データを第1マイクロコンピュータ

に返信するステップと、を含むものである車載制御ユニットの検査方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、車載制御ユニットの検査方法に関するものである。

【0002】

【従来の技術】この種の従来技術として、特開平11-132097号公報の「車両制御用メモリ書き換え装置」がある。同公報の装置は、外部ツールにより電氣的に消去及び書き込み可能な制御メモリ（フラッシュメモリ）を搭載したECU（車載制御ユニット）を備え、書き換え許可された時にのみ前記制御メモリに対するデータ書き換えが実施される。また、この装置は、制御メモリが記憶するソフトウェア（制御プログラム）が正しいことを検査するものであり、その特徴として、

- ・ 予め記憶しておいた制御メモリのサム値（真値）と、ECUで算出したサム値とを共に表示し、それらと比較することで正偽判定を行う。

- ・ 上記サム値の比較は外部ツールの内部で行い、その結果（正偽）のみを返信する。

- ・ イグニッションキースイッチのOFFからONへの切換後にサム値の計算を行う。といった処理を実行する。

【0003】

【発明が解決しようとする課題】上記公報の従来技術では、ECUで計算したサム値を外部ツールに対してそのまま送信する。そのため、ECUと外部ツールとの通信データをモニタすることにより、ECUにより算出した正しいサム値を容易に知り得ることができる。

【0004】また、制御メモリのサム値は、ソフトウェアを書き換えなければ変化しないものであるため、外部チェッカに対して正しいサム値を常に送信するような不正なプログラムを不正改造者が作成し、それをECUに組み込めば、正規のサム値算出アルゴリズムを知らなくても容易に正規ECUとしてなりすますることが可能となる。これは、ECU側で正偽判定を行う構成でも同様である。すなわち、モニタしたサム値を返答する偽プログラムを不正改造者が作成することにより、不正改造された偽ECUであっても、外部ツールは正しいサム値（常に同じ）が返答されたと認識し、正しいECUであると判断してしまう。

【0005】本発明は、上記問題に着目してなされたものであって、その目的とするところは、車載制御ユニットを正しく検査し、ひいては不正改造の防止を図ることができる車載制御ユニットの検査方法を提供することである。

【0006】

【課題を解決するための手段】請求項1に記載の車載制御ユニットの検査方法では、（1）乱数を発生させ、その乱数をサム値の算出指令と共に外部ツールから制御ユ

ニットへ送信する第1のステップ、(2)前記メモリのサム値を算出すると共に、該サム値を前記乱数に応じて暗号化する第2のステップ、(3)前記暗号化したデータを外部ツールに送信する第3のステップ、(4)外部ツールで受信したデータを復号化すると共に、そのデータ中のサム値を予め用意された真のサム値と比較し、その比較判定の結果から車載制御ユニットを検査する第4のステップ、といった各ステップを順に実施するので、不正改造を行おうとする者に正しいサム値が漏れ知れる可能性は低くなる。また、仮に正規の制御ユニットが不正改造され、メモリの正しいサム値を外部ツール側に返信できるような不正なプログラムが制御ユニットに組み込まれたとしても、外部ツールでは、暗号化データを受信すると共にその暗号化データを復号化した後、サム値の比較判定を行うので、不正改造された制御ユニットが正規な制御ユニットとしてなりすますことが極めて困難になる。その結果、車載制御ユニットを正しく検査し、ひいては不正改造の防止を図ることができる。

【0007】上記発明は特に、フラッシュメモリ等、電氣的に書き換え可能な不揮発性メモリにて車載制御ユニット内のメモリが構成される場合に有効である(請求項2)。

【0008】請求項3に記載の発明では、前記第4のステップにおいてサム値が不一致となった場合、前記第1のステップに戻って新たに乱数を設定し、それに続く第2～第4のステップを再度実施する。これにより、一時的な通信異常が原因で正しく検査されなかった場合にも、再通信により適正な検査が実施できる。またここで、乱数を再設定するために制御ユニットと外部ツールとの間の送受信データはその都度異なるので、通信線がモニタされることを想定しても、正しいサム値が漏れ知れる可能性は極めて低くなる。

【0009】請求項4に記載の発明では、

- ・前記第1のステップでは、複数の暗号化アルゴリズムの中から一つを指定してそれを表す識別データを、乱数とサム値の算出指令と共に外部ツールから制御ユニットへ送信し、
- ・前記第2のステップでは、前記識別データによる指定通りの暗号化アルゴリズムを使って暗号化を行い、
- ・その後、前記第4のステップでは、前記指定した暗号化アルゴリズムに対応する復号化の算出式を取り出して受信データを復号化し、サム値を抽出する。

【0010】かかる場合、複数の暗号化アルゴリズムを択一的に使うことにより、不正改造者に暗号化アルゴリズムが知られたとしても、実際に使われた暗号化アルゴリズムに対応させてサム値を解明するのは非常に困難となる。それ故、車載制御ユニットの不正改造を、より一層困難なものとすることができる。

【0011】請求項5に記載の発明では、車載制御ユニットは、電氣的に書き換え可能な不揮発性メモリを実装

した第1マイクロコンピュータと、書き換え不可能なROMを実装した第2マイクロコンピュータとを備え、第2マイクロコンピュータのROMに、前記不揮発性メモリのサム値を暗号化するための暗号化アルゴリズムを記憶させておく。つまり、書き換え不可能な第2マイクロコンピュータのROMにサム値の暗号化アルゴリズムを配置することにより、不正改造防止が更に強化される。

【0012】かかる請求項5の発明では、請求項6に記載したように、第2のステップを実現する上で、前記不揮発性メモリのサム値を第1マイクロコンピュータから第2マイクロコンピュータへ送信するステップと、第2マイクロコンピュータにて前記ROM内の暗号化アルゴリズムでサム値を暗号化した後、その暗号化データを第1マイクロコンピュータに返信するステップと、を設けると良い。

【0013】

【発明の実施の形態】(第1の実施の形態)この発明を具体化した本実施の形態では、エンジン制御等を司るECUにて車載制御ユニットを構成しており、このECUに対して外部ツールを接続し、当該ECUの検査やデータの交換等を行うこととしている。以下、その詳細を図面に従って説明する。

【0014】図1は、制御システムの概略構成を示すブロック図である。本システムにおいて、ECU10は周知のマイクロコンピュータ(以下、マイコンという)11を備え、マイコン11は、予め用意されている制御プログラム等を用いてエンジンの各種制御を実施する。マイコン11は、各種制御の中核をなすCPU12、電氣的に消去及び書き込み可能なフラッシュメモリ13、その他図示しないRAMや入出力回路等を備える。

【0015】外部ツール20も同様に、CPU、メモリ、入出力回路等からなる周知のマイコン21を備える。この外部ツール20は、ECU10の正偽判定等の検査や、同ECU10内のフラッシュメモリ13のデータ書き換えに際し、通信線L1を介してECU10に接続される。これにより、ECU10と外部ツール20との間でシリアル通信によるデータのやり取りが行われる。

【0016】ECU10の正偽判定(検査)の概要を、図2を用いて説明する。かかる場合、フラッシュメモリ13内のデータのサム値と既知の正しいサム値とが比較され、両者が一致すれば、ECU10が正規なものであると判断される。このとき、外部ツール20側では乱数を発生させてそれをECU10に送信する一方、ECU10側では、その内部に予め記憶された暗号化アルゴリズムを用い、サム値を暗号化して外部ツール20に送信するようになっている。なお図2では、処理順序を表すため、(1)～(6)の連続番号を付している。

【0017】先ず始めに、サム値の算出指令と乱数Rtとを含む送信データを通信線L1を介して外部ツール2

0からECU10に送信する(図の(1))。このとき、外部ツール20の送信データは、例えば図5(a)のフレーム構成を有し、このうち、送信ヘッダは送信元ID、送信先ID及びコマンドコードにて構成され、データは送信データID、乱数、本送信データのチェックサム(CS)にて構成されている。

【0018】ECU10側では、フラッシュメモリ13内のデータのサム値Xsumを算出すると共に、所定の暗号化アルゴリズムを用い、乱数Rtに応じてサム値Xsumを暗号化する(図の(2)、(3))。つまり、算出式 $Xt = f(Xsum, Rt)$ により、暗号化したサム値Xt(以下には便宜上、暗号化サム値Xtと言う)を算出する。

【0019】その後、暗号化サム値Xtを通信線L1を介して外部ツール20に送信する(図の(4))。このとき、外部ツール20の受信データは、例えば図5

(b)のフレーム構成を有し、このうち、送信ヘッダは送信元ID、送信先ID及びコマンドコードにて構成され、データは送信データID、暗号化データ、本送信データのチェックサム(CS)にて構成されている。

【0020】外部ツール20では、算出式

$$Xsum = f^{-1}(Xt, Rt)$$

により、暗号化サム値Xtを復号化し、サム値Xsumを算出する(図の(5))。その後、前記の如く算出したサム値Xsumと、予め登録されている真のサム値Xrefとを比較判定する(図の(6))。そして、両者が一致すれば、ECU10が正規ECUであると判断し、不一致であれば、ECU10が偽ECUであると判断する。

【0021】以下には、外部ツール20によるECU10の正偽判定に際し、ECU10及び外部ツール20内の各マイコン11、21により実施される処理の流れを図3及び図4のフローチャートに従い説明する。始めに、外部ツール20の処理の流れを図3のフローチャートで説明する。

【0022】例えば修理工場等において作業者が外部ツール20を操作することで図3の処理がスタートし、先ずステップ101では、乱数発生処理を実行して乱数Rtを設定し、続くステップ102では、コマンド送信を実施する。すなわち、乱数Rtをサム値算出指令と共にECU10に送信する。また、ステップ103ではタイマセットを行う。このステップ101~103が通信前処理に相当する。

【0023】その後、この外部ツール20では、コマンド受信に対するECU10からの受信確認を行う。すなわち、タイムアウトしていないことを条件に(ステップ104がNO)、ステップ105では、前記ステップ102のコマンド送信に対する応答をECU10から受信したか否かを判別する。応答が無いままタイムアウトした場合(ステップ104がYES)、ステップ102に

戻り、再度同じ乱数を用いてコマンド送信を実施する。そして、タイマセット、受信確認の各処理を再び実施する。

【0024】なお、コマンド再送信の回数を予め制限しておき、例えばタイムアウトが3回繰り返されると、通信異常であると判断し、その旨のコードを記憶すると共に以降の処理を中止しても良い。また、1回でもタイムアウトになると、その時点で通信異常と判断しても良い。

【0025】コマンド送信に対する応答を受信すると、ステップ106に進み、以降の受信後処理を実施する。すなわち、ステップ106では、ECU10から受信した暗号化サム値Xtを復号化し、サム値Xsumの生データを抽出する。また、続くステップ107では、予め登録されている真のサム値Xrefを取り出す。

【0026】その後、ステップ108では、サム値Xsum(生データ)と真のサム値Xrefとを比較し、両サム値が一致すると判別されれば(ステップ109がYES)、ECU正常である旨を判断する。

【0027】また、両サム値が不一致であれば(ステップ109がNO)、ステップ110で予め定めた規定回数だけ通信を繰り返したか否かを判別する。NOであればステップ101に戻る。これにより、別の乱数が再設定され、上述した処理が繰り返して実施される。そして、乱数の再設定及びそれに付随するサム値判定の処理が規定回数(例えば3回)だけ繰り返されてもサム値不一致のままであれば、ステップ110がYESとなり、ECU異常である旨を判断する。

【0028】次に、ECU10の処理の流れを図4のフローチャートに従い説明する。先ずステップ201では、外部ツール20よりコマンドを受信したか否かを判別し、YESであればステップ202に進み、受信データから乱数Rtを抽出する。

【0029】その後、ステップ203では、算出式

$$Xsum = \sum Data(i)$$

により、サム値Xsumを算出する。すなわち、フラッシュメモリ13内の規定されたアドレス領域についてアドレスiのデータを全て加算し、その和をサム値Xsumとする。

【0030】その後、ステップ204では、前記受信した乱数Rtでサム値Xsumを暗号化して暗号化サム値Xtを求め、続くステップ205では、暗号化サム値Xtを外部ツール20に送信する。このデータ送信により、外部ツール20では、前記図3のステップ105でデータ受信が確認されることとなる。

【0031】なお本実施の形態では、図3のステップ101、102の処理が本発明の「第1のステップ」に、図4のステップ203、204の処理が「第2のステップ」に、図4のステップ205の処理が「第3のステップ」に、図3のステップ106~109の処理が「第4

のステップ」に、それぞれ該当する。

【0032】以上詳述した本実施の形態によれば、以下に示す効果が得られる。つまり、上記ECU10の検査方法によれば、不正改造を行おうとする者に正しいサム値（算出したサム値Xsum）が漏れ知れる可能性は低くなる。また、仮に正規のECU10が不正改造され、フラッシュメモリ13の正しいサム値を外部ツール20側に返信できるような不正なプログラムが偽ECUに組み込まれたとしても、外部ツール20では、暗号化データを受信すると共にその暗号化データを復号化した後、サム値の比較判定を行うので、不正改造されたECUが正規なECUとしてなりすますことが極めて困難になる。その結果、ECU10を正しく検査し、ひいては不正改造の防止を図ることができる。

【0033】また、サム値不一致の場合、新たに乱数Rtを設定して再検査を行うので、一時的な通信異常が原因で正しく検査されなかった場合にも、再通信により適正な検査が実施できる。またここで、乱数Rtを再設定するためにECU10と外部ツール20との間の送受信データはその都度異なるので、通信線L1がモニタされることを想定しても、正しいサム値が漏れ知れる可能性は極めて低くなる。

【0034】（第2の実施の形態）次に、本発明における第2の実施の形態を説明する。但し、本実施の形態では、上述した第1の実施の形態と同等であるものは説明を簡略化し、第1の実施の形態との相違点を中心に説明する。

【0035】上記第1の実施の形態では不正改造が容認される可能性は極めて低いものの、万が一、暗号化アルゴリズムが不正改造者に漏れ知れた場合、不正改造が可能となる。その対策として、本実施の形態では、複数の暗号化アルゴリズム（算出式）を用意し、そのうちのどのアルゴリズムを使用するかを外部ツール20から指示する方法を提案する。なお本実施の形態では、制御システムとして前記図1の構成をそのまま流用する。

【0036】本実施の形態におけるECU10の正偽判定（検査）の概要を、図6を用いて説明する。なお図6では、処理順序を表すため、（1）～（8）の連続番号を付している。

【0037】先ず始めに、サム値の算出指令と、乱数Rtと、暗号化アルゴリズムの識別コードIDとを含む送信データを通信線L1を介して外部ツール20からECU10に送信する（図の（1））。このとき、外部ツール20の送信データは、例えば前記図5（a）のフレーム構成に対し、データとして暗号化アルゴリズムの識別コードIDを追加した構成となる。

【0038】ECU10側では、フラッシュメモリ13内のデータのサム値Xsumを算出すると共に、外部ツール20からの送信データに含まれる暗号化アルゴリズムの識別コードIDに基づき、それに相応する暗号化の

算出式を取り出す（図の（2）、（3））。また、この算出式を用い、乱数Rtに応じてサム値Xsumを暗号化する（図の（4））。つまり、算出式

$$Xt = f(Xsum, Rt)$$

により、暗号化サム値Xtを算出する。ここで、図示の如く、暗号化IDが0x01, 0x02, … 0x0Fのように与えられる場合、それに対応する算出式はf(*, *), g(*, *), … t(*, *)となり、これら何れかの算出式を用いてサム値Xsumが暗号化される。その後、暗号化サム値Xtを通信線L1を介して外部ツール20に送信する（図の（5））。

【0039】外部ツール20では、その時の暗号化アルゴリズムの識別コードIDに相応する復号化の算出式を取り出し、その算出式にて暗号化サム値Xtを復号化する（図の（6）、（7））。つまり、算出式

$$Xsum = f^{-1}(Xt, Rt)$$

により、サム値Xsumを算出する。

【0040】その後、前記の如く算出したサム値Xsumと、予め登録されている真のサム値Xrefとを比較判定する（図の（8））。そして、両者が一致すれば、ECU10が正規ECUであると判断し、不一致であれば、ECU10が偽ECUであると判断する。

【0041】以下には、外部ツール20によるECU10の正偽判定に際し、ECU10及び外部ツール20内の各マイコン11, 21により実施される処理の流れを図7及び図8のフローチャートに従い説明する。

【0042】始めに、外部ツール20の処理の流れを図7のフローチャートで説明する。但し、図7は前記図3の一部のみを変更したものであり、実際には前記図3そのものに対し、ステップ301, 302の処理を追加したことのみが相違する。以下、前記図3との相違点を中心に説明する。

【0043】図7において、乱数発生処理の後、ステップ301では、多数の暗号化アルゴリズムの中から一つを選択する。そして、続くステップ102では、その暗号化アルゴリズムの識別コードIDを、乱数Rt及びサム値算出指令と共にECU10へ送信する。

【0044】その後、ECU10からの受信確認を終えると、ステップ302では、暗号化アルゴリズムの識別コードIDに対応する復号化の算出式を取り出す。そしてそれ以降、図3で前述した通り、暗号化サム値Xtの復号化、真のサム値Xrefとの比較判定等を行い、ECU10の正偽判定を実施する。

【0045】次に、ECU10の処理の流れを図8のフローチャートに従い説明する。この図8の処理は前記図4に置き換えて実施される。図8では、外部ツール20からのコマンド受信の旨を判別すると、ステップ401からステップ402に進み、受信データから乱数Rtと暗号化アルゴリズムの識別コードID（アルゴリズムNo.）とを抽出する。

【0046】その後、ステップ403では、フラッシュメモリ13内の規定されたアドレス領域についてアドレスiのデータを全て加算し、その和によりサム値Xsumを算出する。

【0047】その後、ステップ404では、指定の暗号化アルゴリズムを取り出し、続くステップ405では、サム値Xsumを暗号化して暗号化サム値Xtを求める。更にステップ406では、暗号化サム値Xtを外部ツール20に送信する。このデータ送信により、外部ツール20では、前記図7のステップ105でデータ受信が確認されることとなる。

【0048】なお本実施の形態では、上記第1の実施の形態との違いとして、図7のステップ301の処理が「第1のステップ」に含まれ、同ステップ302の処理が「第4のステップ」に含まれる。また、図8のステップ402～405の処理が「第2のステップ」に、同ステップ406の処理が「第3のステップ」に、それぞれ該当する。

【0049】以上第2の実施の形態によれば、複数の暗号化アルゴリズムを択一的に使うことにより、不正改造を行おうとする者に暗号化アルゴリズムが知られたとしても、実際に使われた暗号化アルゴリズムに対応させてサム値を解明するのは非常に困難となる。それ故、ECU10の不正改造を、より一層困難なものとすることができる。またこの場合、各々の暗号化アルゴリズムが簡単なものであっても、不正改造者がそのアルゴリズムを認識し、不正改造者両を車検に通す等、不正行為を行おうとすることが困難になる。

【0050】（第3の実施の形態）複雑な制御が要求されるECUには、高い演算負荷を分散させるために複数のマイコン（CPU）を備えて構成されるものがある。例えば2個のマイコンを持つ2マイコンシステムのECUにおいては、前記のフラッシュメモリを搭載し、エンジンの主要制御を受け持つメイン側のマイコンと、制御プログラムを市場で書き換え不可能なROMを搭載し、主要制御以外の制御を受け持つサブ側のマイコンとで構成することがある。

【0051】図9は、本実施の形態における制御システムの概要を示す構成図である。図9の構成では、前記図1の構成との違いとして、ECU30は、第1マイコン（第1マイクロコンピュータ）31と第2マイコン（第2マイクロコンピュータ）32とを備える。第1マイコン31は、燃料噴射制御や点火時期制御等、エンジンの主要な制御を受け持つマイコンであり、CPU31aとフラッシュメモリ31bとを実装する。また、第2マイコン32は、トランスミッション制御等を受け持つマイコンであり、CPU32aと、プログラムを市場で書き換え不可能なROM32bとを実装する。

【0052】こうした2マイコンシステムのECU30において、第2マイコン32のROM32b内には、第

1マイコン31の正偽判定を行うために用いる暗号化アルゴリズムが格納されている。

【0053】図10は、第1マイコン31の処理と第2マイコン32の処理とを個々に示すフローチャートである。先ずは、図10（a）に従い、第1マイコン31の処理の流れを説明する。

【0054】図10（a）では、外部ツール20からのコマンド受信の旨を判別すると、ステップ501からステップ502に進み、受信データから乱数Rtを抽出する。その後、ステップ503では、フラッシュメモリ31b内の規定されたアドレス領域についてアドレスiのデータを全て加算し、その和によりサム値Xsumを算出する。その後、ステップ504では、前記受信した乱数Rtと、前記算出したサム値Xsumとを第2マイコン32に送信する。

【0055】続くステップ505では、第2マイコン32へのデータ送信に回答して当該第2マイコン32からデータ受信をしたか否かを判別する。この受信データには、第2マイコン32で暗号化された暗号化サム値Xtが含まれており、データ受信を確認した後、ステップ506では、暗号化サム値Xtを外部ツール20に送信する。このデータ送信により、外部ツール20では、前記図3のステップ105でデータ受信が確認されることとなる。

【0056】次に、第2マイコン32の処理の流れを図10（b）のフローチャートに従い説明する。図10（b）では、前記図10（a）のステップ504におけるデータ送信を伴い、第1マイコン31からのデータ受信の旨を判別すると、ステップ601からステップ602に進み、受信データから乱数Rtとサム値Xsumとを抽出する。その後、ステップ603では、ROM32b内に用意されている所定の暗号化アルゴリズムを用い、サム値Xsumを暗号化して暗号化サム値Xtを求める。続くステップ604では、暗号化サム値Xtを第1マイコン31に送信する。このデータ送信により、第1マイコン31では、前記図10（a）のステップ505でデータ受信が確認されることとなる。そして更に、このデータが外部ツール20に送信される。

【0057】なお本実施の形態では、上記第1の実施の形態との違いとして、図10（a）のステップ503、504及び図10（b）のステップ603の処理が「第2のステップ」に、図10（a）のステップ506の処理が「第3のステップ」に、それぞれ該当する。

【0058】以上第3の実施の形態によれば、第2マイコン32のROM32bに暗号化アルゴリズムを記憶させておくので、暗号化アルゴリズムを不正に書き換えることが不可能となり、不正改造防止が更に強化される。

【0059】上記第3の実施の形態では、第2マイコン32のROM32bに所定の暗号化アルゴリズムを記憶させる構成であったが、この構成を変更しても良い。例

例えば、既述した第2の実施の形態のように、第2マイコン32のROM32bに複数の暗号化アルゴリズムを記憶させておき、外部ツール20から指定される識別コードに従い、複数の暗号化アルゴリズムの中から一つを選択する構成としても良い。

【0060】また、同じく第3の実施の形態では、外部ツール20から送信される乱数 R_t を一旦第1マイコン31で受信し、その後、サム値と共に第2マイコン32へ転送したが、この乱数 R_t を外部ツール20から第2マイコン32へ直接送信する構成としても良い。

【図面の簡単な説明】

【図1】 発明の実施の形態における制御システムの概略構成を示すブロック図。

【図2】 ECUの正偽判定の様子を示す説明図。

【図3】 外部ツールの処理の流れを示すフローチャート。

【図4】 ECUの処理の流れを示すフローチャート。

【図5】 送信データ及び受信データのフレーム構成を示す図。

【図6】 第2の実施の形態においてECUの正偽判定の様子を示す説明図。

【図7】 第2の実施の形態において外部ツールの処理の流れを示すフローチャート。

【図8】 第2の実施の形態においてECUの処理の流れを示すフローチャート。

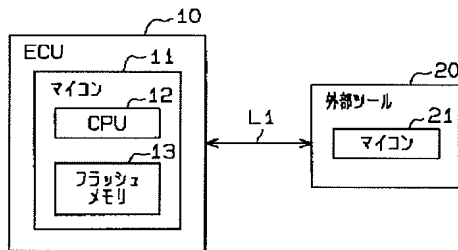
【図9】 第3の実施の形態において制御システムの概略構成を示すブロック図。

【図10】 第3の実施の形態において第1マイコン及び第2マイコンの処理の流れを示すフローチャート。

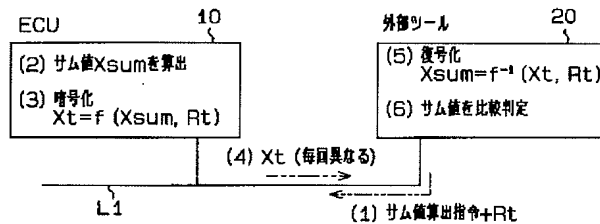
【符号の説明】

10…ECU、11…マイコン、12…CPU、13…フラッシュメモリ、20…外部ツール、30…ECU、31…第1マイコン、31b…フラッシュメモリ、32…第2マイコン、32b…ROM。

【図1】



【図2】



【図5】

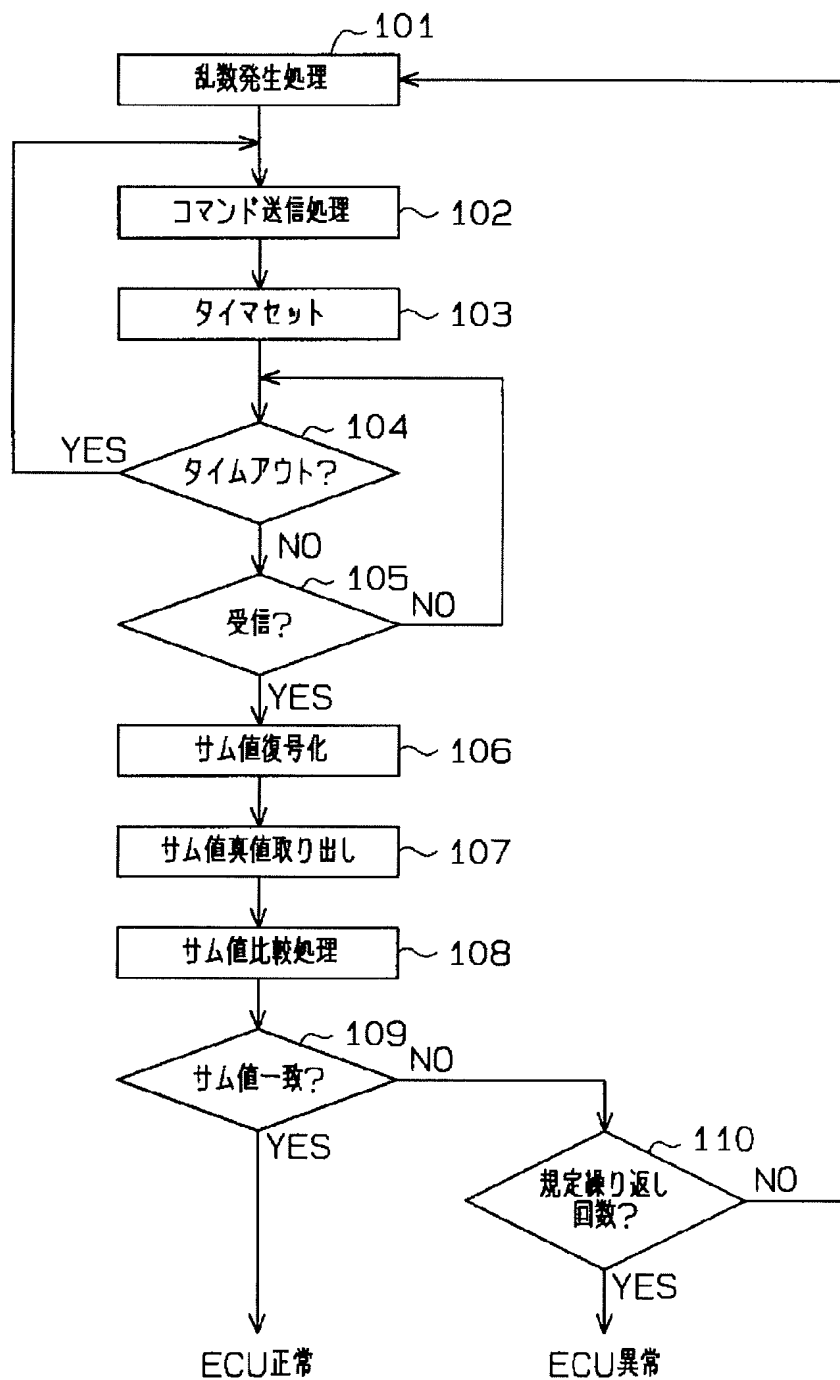
(a) 送信データの例

送信ヘッダ (送信元ID、送信先ID、コマンドコード)	データ (送信データID、乱数、CS)
--------------------------------	------------------------

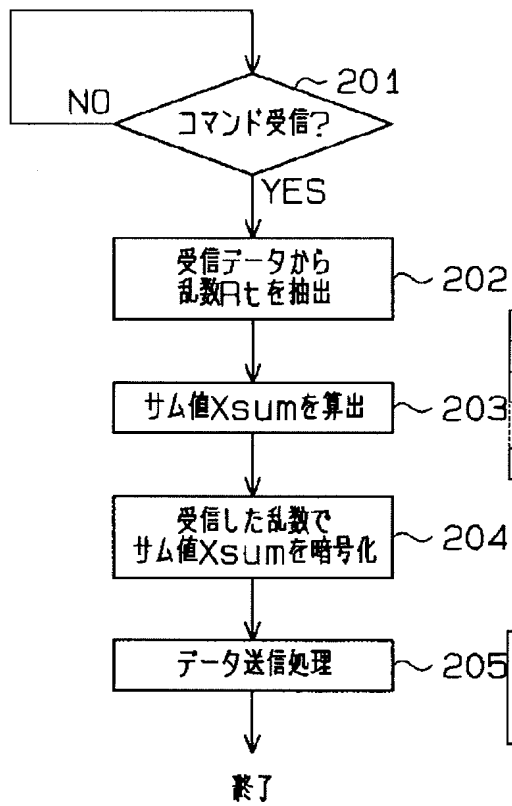
(b) 受信データの例

送信ヘッダ (送信元ID、送信先ID、コマンドコード)	データ (送信データID、暗号化データ、CS)
--------------------------------	----------------------------

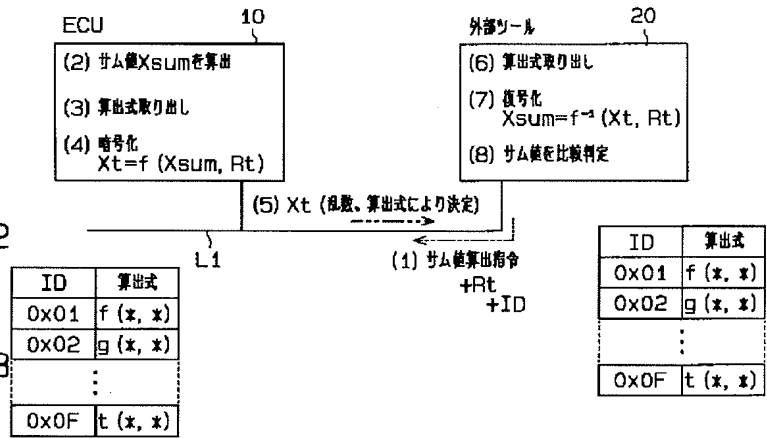
【図3】



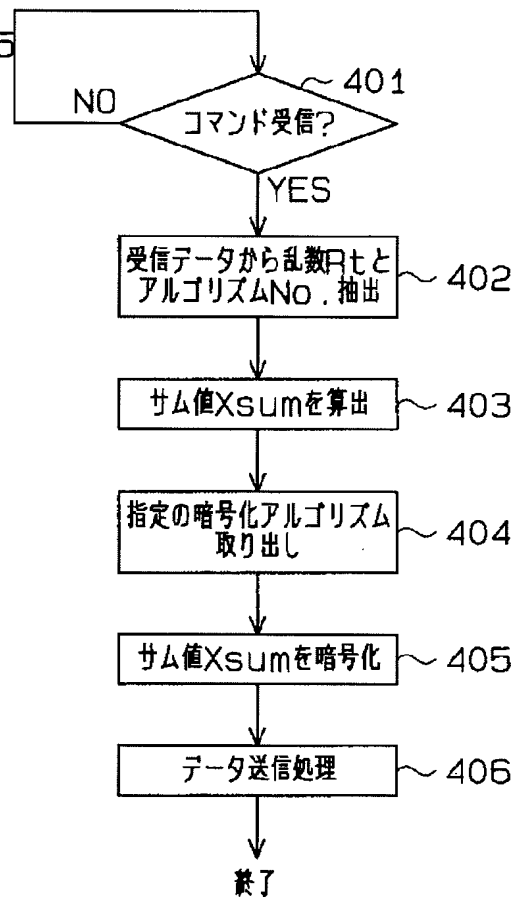
【図4】



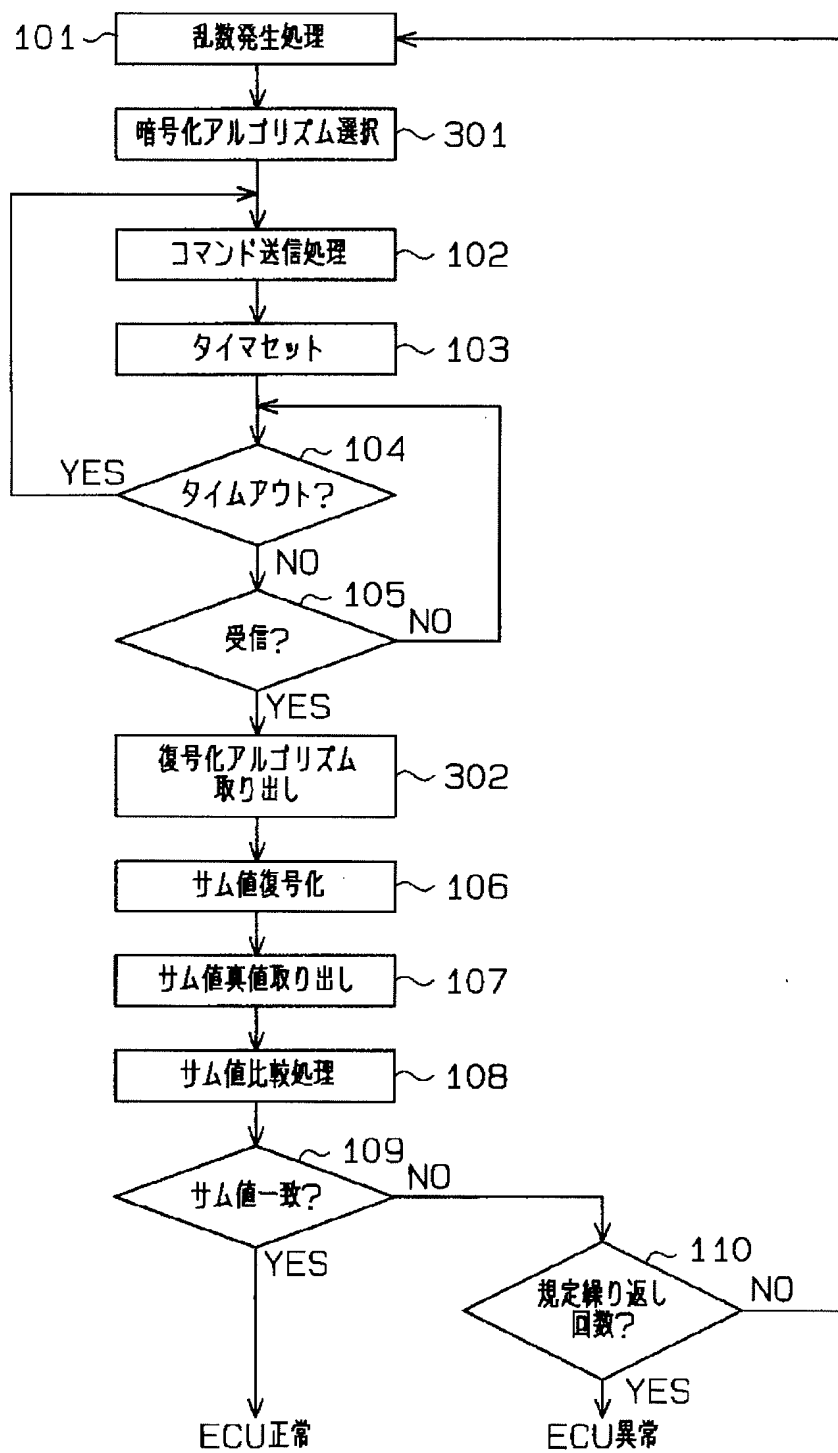
【図6】



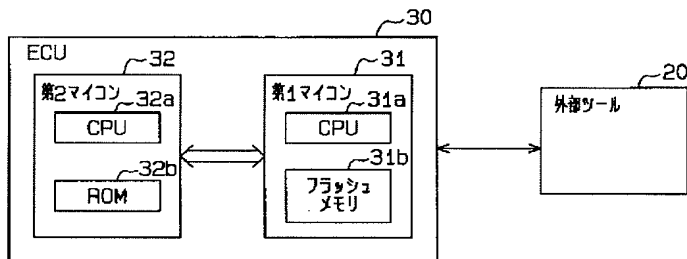
【図8】



【図7】

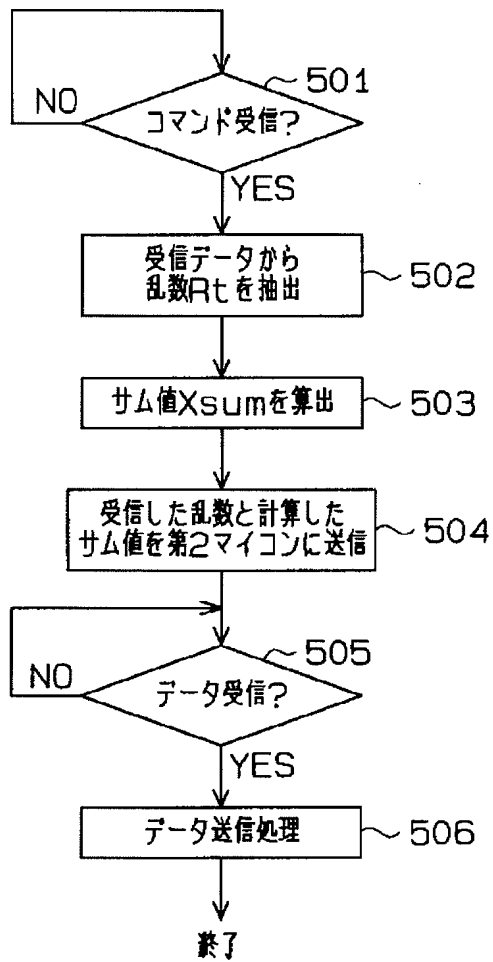


【図9】

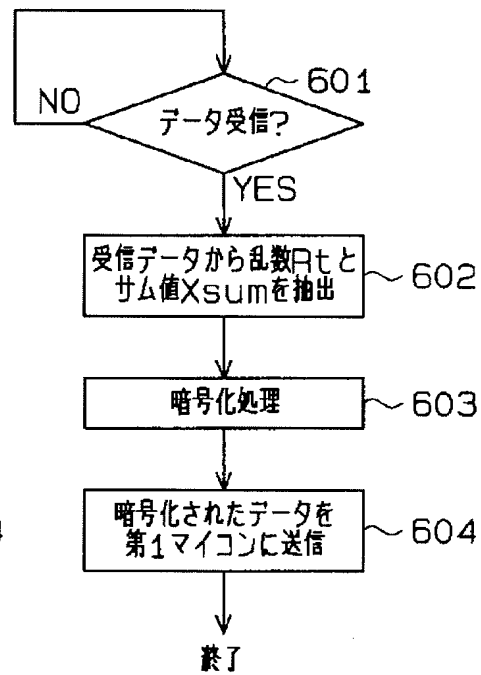


【図10】

(a) 第1マイコンの処理



(b) 第2マイコンの処理



フロントページの続き

(72)発明者 青木 千鶴

愛知県刈谷市昭和町1丁目1番地 株式会
社デンソー内

Fターム(参考) 5B048 AA14 CC02 DD06